Элементы теории Галуа.

Терминология. Конечное расширение $\Bbbk \subset \mathbb{F}$ называется *расширением Галуа*, если $\dim_{\Bbbk}\mathbb{F} = |\mathrm{Aut}_{\Bbbk}\mathbb{F}|$. Группа $\mathrm{Aut}_{\Bbbk}\mathbb{F}$ называется в этом случае *группой Галуа* $\mathbb{F}$ над $\Bbbk$ и обозначается $\mathrm{Gal}\,\mathbb{F}/\Bbbk$. Группа Галуа $\mathrm{Gal}\,f/\Bbbk$ многочлена $f \in \Bbbk[x]$ — это группа Галуа его поля разложения. Мы полагаем $\sqrt[n]{1} = e^{\frac{2\pi i}{n}} \in \mathbb{C}$.

A16◇1. Пусть $\Bbbk \subset \mathbb{F}$ — расширение Галуа с группой Галуа G. Покажите, что

а) $\exists\, \vartheta \in \mathbb{F}$, G-орбита которого есть базис $\mathbb{F}$ как векторного пространства над $\Bbbk$.

б) все $f \in \Bbbk[x]$, имеющие в $\mathbb{F}$ корень, полностью разлагаются там на линейные множители.

A16◇2. Покажите, что при $\mathrm{char}\,\Bbbk \neq 2$ группа Галуа многочлена $f \in \Bbbk[x]$ осуществляет лишь чётные перестановки его корней, если и только если $D(f)$ является квадратом в $\Bbbk$.

A16◇3. Найдите группу Галуа над $\mathbb{Q}$ многочленов **а)** x^3-3x+1 **б)** x^3+2x+1 **в)** x^4-5x^2+6 **г)** x^4+x^2+1 **д)** x^4+1 и выразите их корни через квадратные и кубические радикалы.

A16◇4. Предъявите угол, который нельзя разбить на три равных угла циркулем и линейкой.

A16◇5. Найдите группу Галуа над $\mathbb{Q}$ поля **а)** $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ **б)** $\mathbb{Q}(\sqrt[3]{1}+\sqrt[3]{2})$ **в)** полученного присоединением к $\mathbb{Q}$ всех $\sqrt[7]{5}$. Опишите все подполя этих полей и вычислите группу Галуа над $\mathbb{Q}$ тех, что являются расширениями Галуаполя $\mathbb{Q}$.

A16◇6*. Найдите группу Галуа над $\mathbb{Q}$ многочлена x^4+2x^2+x+3.

A16◇7*. Предъявите $f \in \mathbb{Z}[x]$ с $\deg f = 6$ и $\mathrm{Gal}\,f/\mathbb{Q} \simeq S_6$.

A16◇8. Выразите **а)** $\sqrt[5]{1}$ **б)** $\sqrt[17]{1}$ через квадратные корни, а **в)** $\sqrt{13}$ через $\sqrt[13]{1}$

A16◇9. Пусть $p > 2$ — простое, $\mathbb{F} = \mathbb{Q}[\sqrt[p]{1}]$. Покажите, что $G = \mathrm{Gal}\,\mathbb{F}/\mathbb{Q}$ содержит единственную подгруппу индекса 2 и опишите соответствующее квадратичное расширение $\mathbb{Q}$.

A16◇10. Пусть $p \in \mathbb{N}$ — простое, и $a \in \mathbb{Q}$ не является p-той степенью. Покажите, что группа Галуа многочлена $x^p - a$ над $\mathbb{Q}$ изоморфна группе аффинно-линейных автоморфизмов аффинной прямой над $\mathbb{F}_p$.

A16◇11* (квадратичный закон взаимности). Пусть $p, q > 2$ — простые. Положим $q^* = (-1)^{\frac{q-1}{2}}q$, $\mathbb{K} = \mathbb{Q}[\sqrt{q^*}]$ и $O \subset \mathbb{K}$ подкольцо всех его целых над $\mathbb{Z}$. Покажите, что:

а) $[q^*]_p$ квадрат в $\mathbb{F}_p \iff O/(p) = \mathbb{F}_p \oplus \mathbb{F}_p \iff$ автоморфизм Фробениуса $\varphi_p : z \mapsto z^p$ тождественно действует на $O/(p)$ (кстати, какова альтернатива 2-го и 3-го условий?)

б) существует вложение полей $\mathbb{K} \hookrightarrow \mathbb{Q}[\sqrt[q]{1}] \subset \mathbb{C}$, такое что действие φ_p является приведением по модулю p ограничения на O отображения $\mathbb{C} \xrightarrow{z\mapsto z^p} \mathbb{C}$.

в) Получите явное выражение $\sqrt{q^*}$ через корни q-той степени из единицы, выясните как действует на него возведение в p-тую степень (по модулю p), и установите квадратичный закон взаимности[1]: $[p/q]\cdot[q/p] = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

A16◇12. Постройте правильный 17-угольник циркулем и линейкой.

A16◇13. Покажите, что **а)** $\mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\sqrt[4p]{1}]$ при простом $p \equiv 3 \pmod 4$

б) любое квадратичное расширение $\mathbb{Q}$ содержится в некотором круговом поле $\mathbb{Q}[\sqrt[m]{1}]$.

A16◇14. Пусть $u = p(t)/q(t)$, где $p, q \in \Bbbk[t]$ взаимно просты. Покажите, что:

а) $\dim_{\Bbbk(u)}\Bbbk(t) = \max(\deg p, \deg q)$

б) $\mathrm{Aut}_{\Bbbk}\Bbbk(t) = \mathrm{PGL}_2(\Bbbk)$ это группа дробно линейных замен переменной t.

A16◇15. Пусть $G = \mathrm{PGL}_2(\mathbb{F}_q)$, а $P \subset G$ и $N \subset P$ состоят из замен $t \mapsto at+b$ (с $a \neq 0$) и $t \mapsto t+b$. Покажите, что подполя инвариантов этих групп в $\mathbb{F}_q(t)$ суть

а) $\mathbb{F}_q(t)^N = \mathbb{F}_q(t^q - t)$ **б)** $\mathbb{F}_q(t)^P = \mathbb{F}_q\left((t^q-t)^{q-1}\right)$ **в)** $\mathbb{F}_q(t)^G = \mathbb{F}_q\left(\frac{\left(t^{q^2}-t\right)^{q+1}}{(t^q-t)^{q^2+1}}\right)$

A16◇16*. Покажите, что алгебраическое замыкание $\mathbb{F}_p$ получается присоединением к $\mathbb{F}_p$ всех примитивных корней из единицы всех простых степеней, отличных от p.

[1] напомним, что *символ Лежандра–Якоби* $[n/p]$ равен -1, если n не квадрат по модулю p, 0, если n делится на p, и 1 в остальных случаях